Modernization Partner

United States Department of Education
Student Financial Assistance

Internet Security Standards

Task Order # 4

Deliverable # 4.1.3

February 16, 2000

Contents

Department of Education

SFA needs to build a security architecture and develop security competencies to support the SFA business initiatives

Department of Education

The SFA security environment, currently consisting of various computing environments with a variety of security technology and practices, is in need of integrated security architecture services that provide a secure environment to enable SFA strategic initiatives. The security architecture should take advantage of security best practices to ensure customer and business partner confidence in the security of SFA data and to support the requirements of SFA business initiatives.

A major SFA security concern is the privacy and authenticity of information. Students, schools, business partners and employees need to be confident that:

- data cannot be stolen or improperly disclosed
- documents that are signed by an individual actually originated from that individual
- transactions can be traced to the individuals, institutions and / or processes that initiated the transaction
- individuals cannot repudiate or deny transactions that they initiate or authorize

This document lays the foundation for building the security strategy and competencies needed within SFA to support the business initiatives. This document identifies the major SFA security requirements that support the business initiatives, links these security requirements to security architecture services, and identifies gaps in the current security architecture that need to be bridged to support the SFA business initiatives.

Inputs to the Recommendation Process

Department of Education

In defining security recommendations, we relied on:

- SFA personnel
- SFA Guiding Principles & Security Requirements--as established in project EASI and the Modernization Blueprint
- Existing SFA business processes and technology
- Andersen Consulting's security architecture best practices and prior implementation experience

Objectives

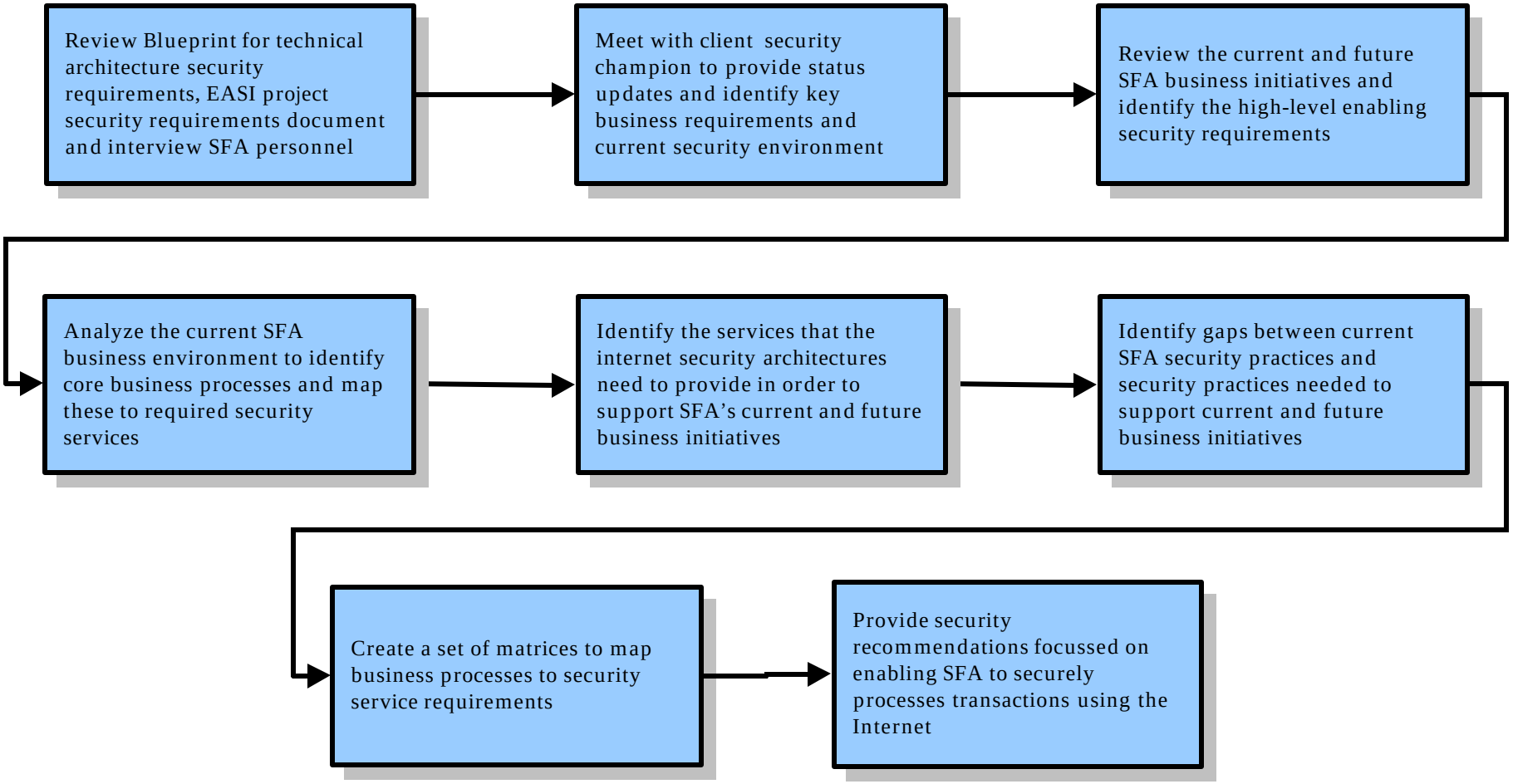
Department of Education

The objectives of Task Order # 4, Deliverable # 4.1.3, Internet Security Standards were to:

- Present the impact and importance that security has on conducting business in the Internet environment
- Identify security concerns associated with the major business processes
- Construct a team to develop security solutions that address the identified security concerns
- Recommend a general security & privacy architecture
- Provide a framework that identifies security areas and components to be included in the design of a comprehensive security & Privacy architecture

The following diagram outlines the project approach for Deliverable # 4.1.3: Internet Security Standards

Department of Education

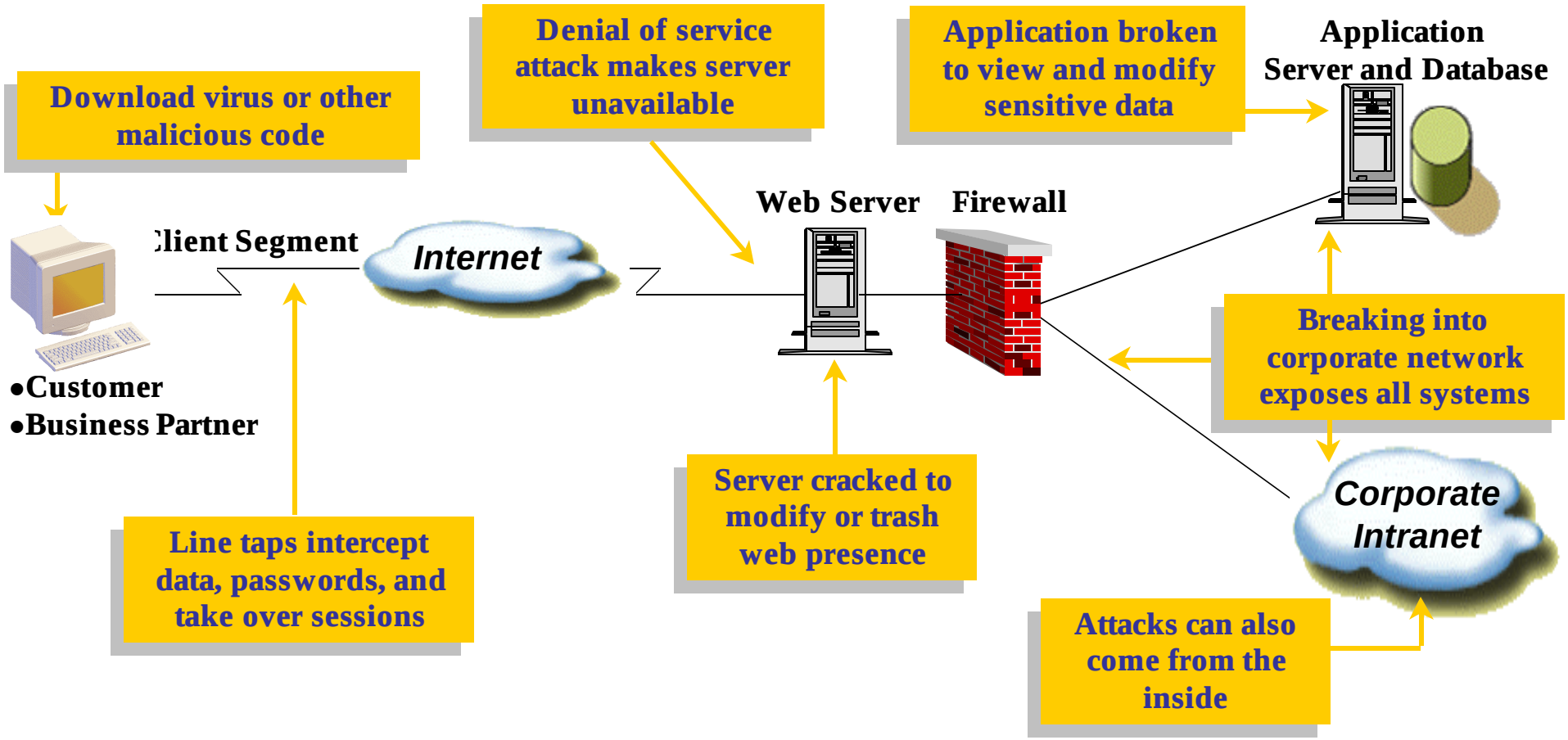


Contents

Department of Education

Conducting business on the Internet opens networks to additional security threats and business liabilities that are not always present in an intranet environment

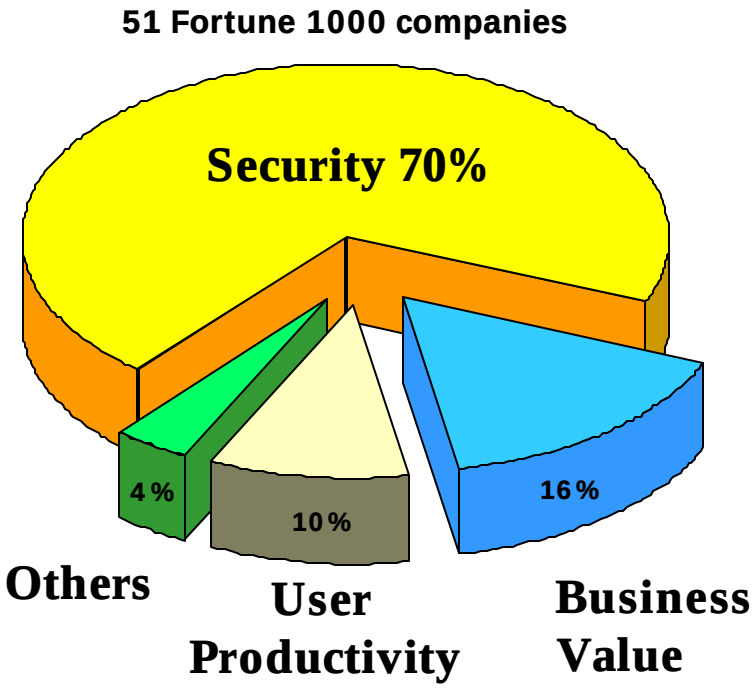
Department of Education



Recent surveys show that commercial business have similar Internet security concerns as SFA

Department of Education

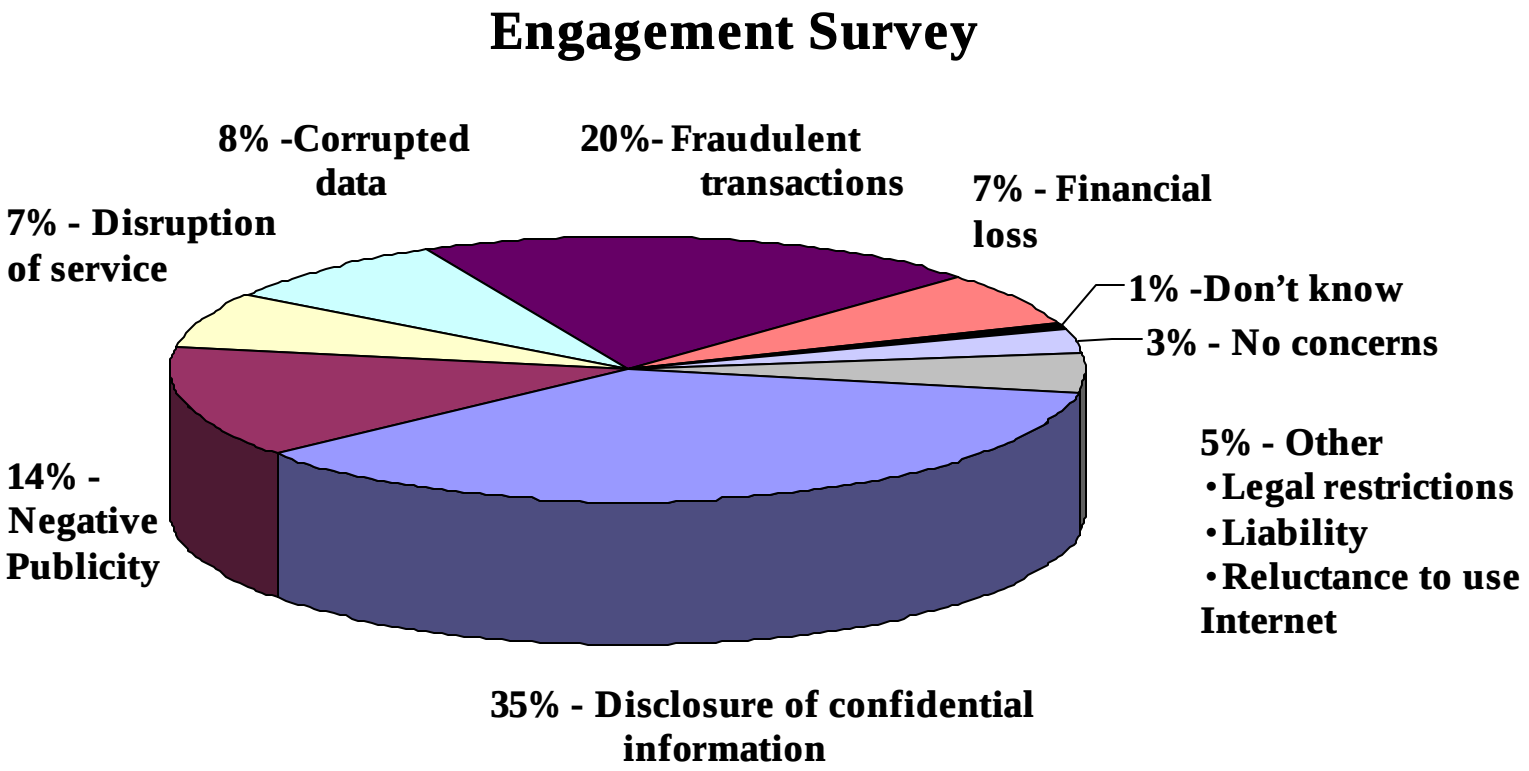
What are your top three Internet issues?



Recent surveys show that disclosure of confidential information, fraudulent transactions and negative publicity are the most common concerns in the Internet business environment

Department of Education

Q: What were the project team's most important security concerns?



Contents

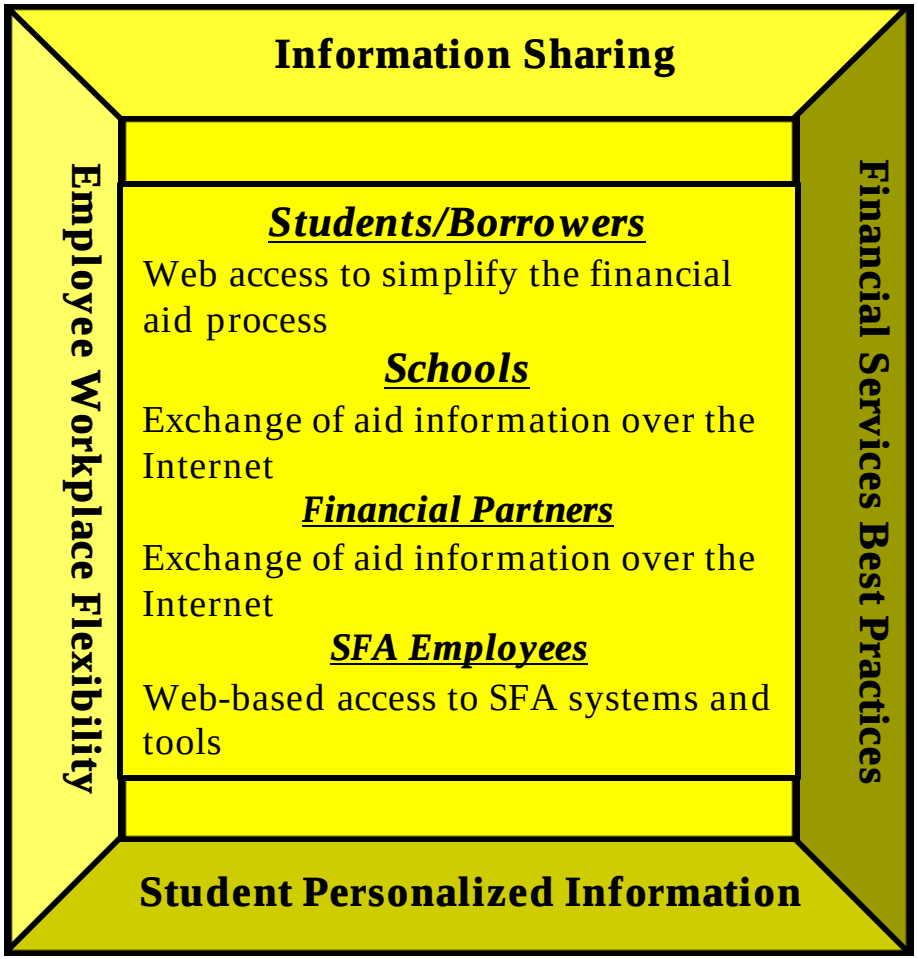
Department of Education

- **Introduction**
  - Objectives
  - Approach
- **Internet Security Challenges**
  - Internet Security Threats
  - Recent Security Surveys
- **SFA Security Challenges**
  - Business Imperatives
  - Security Issues & Concerns
  - Current Security Practices & New Requirements
- **Security Requirements**
  - Security Services / Business Processes Matrix
  - Security Services / Security Solutions Matrix
  - Security Services / Stored Information Matrix
- **SFA Security Initiative**
  - Security Imperatives
  - Security Framework
- **Next Steps**
  - Security Guiding Principles
  - Security Projects

The SFA business imperatives drive the requirements for a new security approach

Department of Education

SFA Business Imperatives



SFA Security Requirements

Secure Web Server, Hosts & Data

- Ensure that Web server and hosts operate continuously
- Information is not modified without authorization
- Information is only distributed to authorized individuals

Secure In-transit Information

- Information that the user supplies to the server cannot be read, modified, or destroyed by others while in transit

Build User Confidence

- Users know that their information stored on SFA systems is secure
- Users know that data, information or programs downloaded from SFA do not cause damage to their systems

SFA's technology architecture must respond to security concerns and customer needs in the Internet, intranet and extranet environments

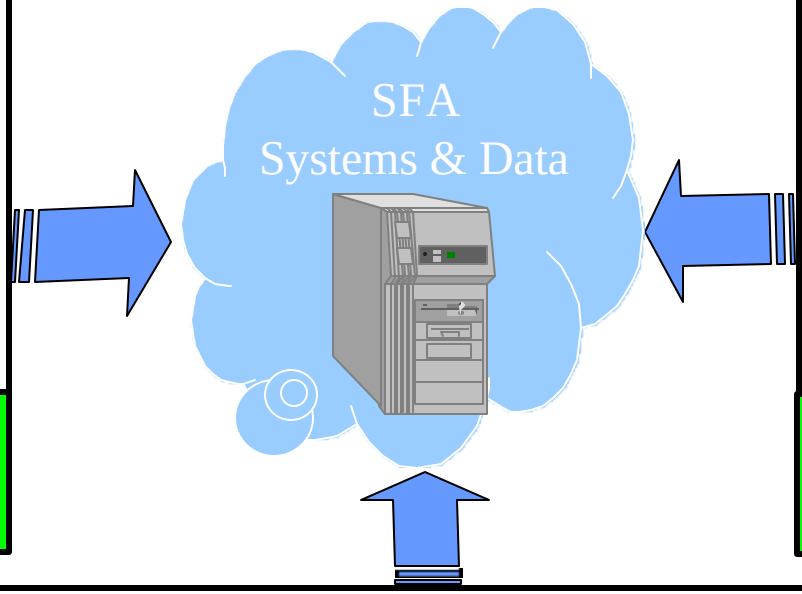
Department of Education

SFA Security Issues & Concerns

Internet Users

- 30 million customers (applicants, students, and borrowers) access SFA systems via the Internet
- Users are increasingly provided with view and update access to their own data
- Certain users need view and update access to other customers' private data

Major Concerns Are Data Confidentiality And Accessibility



Intranet Users

- Approximately 3,000 Department of Education employees and contractors access SFA systems over dedicated or dial-up telecommunication lines
- Many users have privileged access to SFA machines, and can modify systems and data

Major Concerns Are Access Restrictions to Data & Systems

Extranet Users

- Approximately 13,000 officials and computer systems at state agencies, guarantee agencies and schools send data directly to SFA system processing queues, generally via TIV WAN
- TIV WAN access will be replaced over the next 2 years with Internet connectivity
- Some users are able to change SFA data and trigger funds transfers, subject to application system edits and written agreements

Major Concerns Are Authentication, Authorization And Transaction Logging

SFA has an identification and authentication infrastructure, but the SFA approach to identification and authentication is neither coordinated or comprehensive

Department of Education

Current SFA Security Practices

- Each system has its own security technology with limited consistency between different security systems
- Application and operating system based security is used to control and log access of all authorized users
  - Operating system access controls rely only on user ID and password (which can be easily subverted) for user identification and authentication
  - Database security defines the type of access allowed to data
  - Application security limits the functions that users can perform based on business rules
- The ePIN is used to authenticate users accessing the SFA systems via the Internet
- SFA provides customer assurance of data privacy for transactions submitted via the Internet
  - Student/borrower financial aid data transmitted via the internet are encrypted using SSL

New SFA Security Requirements

- Strong identification and authentication services should be provided for users accessing SFA systems via the Internet
  - Access to private information should be allowed only after determining that the user is identified, authenticated and authorized to access that data. Options to consider include authentication servers, directory services, certificates, smartcards, one-time passwords.
- Strong network perimeter security should be implemented to protect SFA's information assets from unauthorized access from the Internet
  - Options to consider include firewall, web access control software, intrusion detection software
- SFA needs to provide digital notarization and non-repudiation
  - Digital signatures should be used to verify the authenticity of documents and senders

SFA has a limited security architecture, but a comprehensive security architecture is needed to meet the Internet challenges. The following pages describe the security services that SFA needs for a secure Internet environment.

Contents

Department of Education

- **Introduction**
  - Objectives
  - Approach
- **Internet Security Challenges**
  - Internet Security Threats
  - Recent Security Surveys
- **SFA Security Challenges**
  - Business Imperatives
  - Security Issues & Concerns
  - Current Security Practices & New Requirements
- **Security Requirements**
  - Security Services / Business Processes Matrix
  - Security Services / Security Solutions Matrix
  - Security Services / Stored Information Matrix
- **SFA Security Initiative**
  - Security Imperatives
  - Security Framework
- **Next Steps**
  - Security Guiding Principles
  - Security Projects

Security services that are needed by SFA business processes

Department of Education

The first step in developing a secure netcentric environment is to understand the business processes that are performed. Once the main processes are documented, they can be analyzed to better understand the security services that are required to securely perform these processes.

A business process refers to one of the main tasks currently performed by SFA, and potentially, by a new system.

Security services required by a business process

Business Process	Confidentiality	Identification	Authentication	Authorization	Accountability	Integrity	Non-Repudiation
Students							
View financial aid research and planning						X	
Sign FAFSA		X	X		X		X
Submit FAFSA	X	X	X	X	X	X	
Sign promissory Note	X	X	X	X	X	X	X
View own SFA account	X	X	X	X		X	
Change / Update own SFA account	X	X	X	X	X	X	
Request for forbearance of deferment	X	X	X				X
Apply for loan consolidation	X	X	X				X

Note: Security services are explained at page 22

Security services that are needed by SFA business processes (contd.)

Department of Education

Business Process	Confidentiality	Identification	Authentication	Authorization	Accountability	Integrity	Non-Repudiation
Schools							
View SFA forms and guidelines						X	
View student SFA account	X	X	X	X		X	
Change / Update student SFA account	X	X	X	X	X	X	
Update student enrollment status		X	X	X		X	
Send Promissory Note to lender	X	X	X	X		X	
Schools submit audited financial statements	X	X	X	X			X
Submit QA reports		X	X	X			
Receive notification of cohort default rates CDR	X	X	X	X			
Receive CDR guide		X	X	X			
Receive loan record detail reports	X	X	X	X			
Submit CDR appeals		X	X	X			
Receive notification of CDR appeal determination		X	X	X			
Submit copy of all accrediting decisions		X	X				
Submit copy of most recent directory of accredited institutions		X	X				
Submit copy of accredidation standards		X	X				
Financial Partners							
View SFA forms and guidelines						X	
View student SFA account	X	X	X	X		X	
Review and accept application	X	X	X	X	X	X	X
Review and accept promissory note	X	X	X	X	X	X	X
Transfer funds to schools	X	X	X	X	X	X	
Update student loan balances	X	X	X	X	X	X	

Security Solutions that fulfill Security Service Requirements

Department of Education

Once the major security concerns have been established and their importance evaluated, security solutions can be chosen that best address these concerns. Many times a combination of solutions is needed.

A Security service requirement refers to an area of concern (i.e. information confidentiality) when business processes are performed

A security solution refers to a range of products that are provided by the security market to fulfill security services

Security Service Required	Security Solution						
	Digital Certificates	Firewall	Encryption	Intrusion Detection	Security Monitoring Software	Access Control	Vulnerability Tools
Confidentiality			X				
Identification	X	X					
Authentication	X	X					
Authorization						X	
Accountability	X			X	X		
Integrity	X			X	X		X
Non-Repudiation	X						

Security Requirements - Security Services / Stored Information Matrix

Information privacy requirements drive the security protection needed for students', borrowers' and business partners' data stored in SFA systems

Department of Education

Information Class	Information Type	Identification	Authentication	Authorization	Accountability	Integrity	Non-Repudiation
Financial Aid	Business & Personal	☑	☑	☑		☑	
Transactions & Repayments	Business & Personal	☑	☑	☑	☑	☑	
FAFSA	Personal	☑	☑	☑		☑	
Schools	Business					☑	
Packages	Business & Personal	☑	☑	☑		☑	
Participants	Personal	☑	☑	☑		☑	
Promissory Notes	Business & Personal	☑	☑	☑	☑	☑	☑
Organization Information	Business	☑	☑	☑		☑	
Customer Service	Business					☑	
Organization Review Information	Business					☑	
School Enrollment	Business & Personal	☑	☑	☑		☑	
Management Information	Business					☑	

SFA Information Assets

Information Type

Personal- Requires security services that will protect the privacy and integrity of personal information for financial aid applicants and borrowers

Business- Requires security services that will protect the privacy and integrity of sensitive business data for SFA and business partners (Guarantors, Schools, Lenders, State Grant Agencies)

Information Class Description

Financial Aid: Award, repayment, collection, consolidation and participant (e.g. student, parent), status change, discharge

Transactions & Repayments: Funds awarded, disbursements and repayments

FAFSA: Financial aid application, applicant and/or borrower income

Schools: Financial aid program dollar amounts designated for each school, financial information, program participation agreement

Packages: Financial aid packages information

Participants: Information about borrower's personal and financial history

Promissory Notes: Detailed information about the borrowing agreement

Organization Information: Performance rating, accrediting and licensing information

Customer Service: SFA information relating to CRM activities

Organization Review Information: Details of school financial aid program review

School Enrollment: Enrollment information about applicants/borrowers

Management Information: Program document information

Contents

Department of Education

- **Introduction**
  - Objectives
  - Approach
- **Internet Security Challenges**
  - Internet Security Threats
  - Recent Security Surveys
- **SFA Security Challenges**
  - Business Imperatives
  - Security Issues & Concerns
  - Current Security Practices & New Requirements
- **Security Requirements**
  - Security Services / Business Processes Matrix
  - Security Services / Security Solutions Matrix
  - Security Services / Stored Information Matrix
- **SFA Security Initiative**
  - Security Imperatives
  - Security Framework
- **Next Steps**
  - Security Guiding Principles
  - Security Projects

The SFA business imperatives drive security requirements that determine the SFA security initiatives

Department of Education

SFA Business Imperatives

- ✓ Secure Internet access to SFA Systems & data for customers, business partners, and SFA employees and contractors
- ✓ Secure and seamless Internet interface between SFA and business partners' systems
- ✓ Information privacy for customers and business partners

Objectives

SFA Security Requirements

- Identification, Authentication & Authorization
- Information Confidentiality & Availability
- Transaction Integrity & Non-repudiation
- Transaction Auditing & Logging

SFA Security Initiatives

- ✓ Security & privacy organization
- ✓ Security & privacy policies and procedures that guide the SFA organization
- ✓ Security & Privacy Framework that defines standards
- ✓ Security & privacy architecture that implements standards

Strategies

Description of security services that are most applicable to the SFA internet environment

Department of Education

There are many security solutions currently available, but understanding which ones best fit the needs of SFA's business processes is seldom easy. By establishing security service requirements, the most applicable security solutions can be effectively selected and implemented.

The major security services that need to be addressed in SFA are:

- ***Confidentiality*** is the concept of protecting sensitive data from improper disclosure while in storage or in transit. Encryption is used to protect information confidentiality during transmission or storage.
- ***Authentication*** is the process of identifying and ensuring that an entity is who it claims to be. For individuals, authentication is usually based on a username and password. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Individual access rights are addressed by the authorization services
- ***Authorization*** is the process of granting or denying access to a resource (i.e., application server, printer, remote access server, Internet, etc.). Within this context, authorization includes the process of initially verifying identity and setting up access as well as the system functions of granting or denying access to resources.
- ***Accountability*** is the ability to associate a transaction in the system with a specific user identifier.
- ***Integrity*** is the concept that ensures that information processed, stored, or transmitted between systems or network components is accurate and complete.
- ***Non-Repudiation*** is the concept of providing tamperproof evidence that a specific action or transaction has occurred. Non-repudiation services should be able to produce legally binding evidence. This service is commonly implemented in financial systems where electronic transactions take place.

A security framework describes security areas and components to be considered when designing a security architecture

Department of Education

To ensure information security and protect the business assets of SFA, all areas of the security architecture (people, process and technology) should work together as part of the security solution. Use of a security framework during the plan, design, build and operations phases of the SFA security architecture will ensure integration of people, process and technology. The security framework can be summarized as the following three areas:

- **Business Assets, Security Strategy and Risk Management** – form the core of the model.
  - ***Business Assets*** represent what needs protection, and is the target of all information security efforts.
  - ***Risk Management*** - analyzes the ***Business Assets'*** value and the cost to protect the assets, identifies the level of protection required, and discovers the threats and vulnerabilities that must be addressed through the *Security Strategy.*
  - ***Security Strategy*** - defines the conceptual approach and direction the organization is taking to secure the *Business Assets* at a business capability level.
- **Core Capabilities** – include *Security Management, Security Administration, Security Operations, Security Awareness, Security Policy & Standards, Security Development, and Security Compliance.* Core Capabilities are the security functions performed by people to provide a desired level of information security. The level of information security provided is determined by the *Risk Assessment.*
- **Technology Architecture** - consists of the *Security Infrastructure* and *Security Services* that protect the ***Business Assets***. Together with the **Core Capabilities**, the Technology Architecture provides the protective tools and services that help achieve the ***Security Strategy***.

Refer to the ***"Security Framework"*** for detailed descriptions

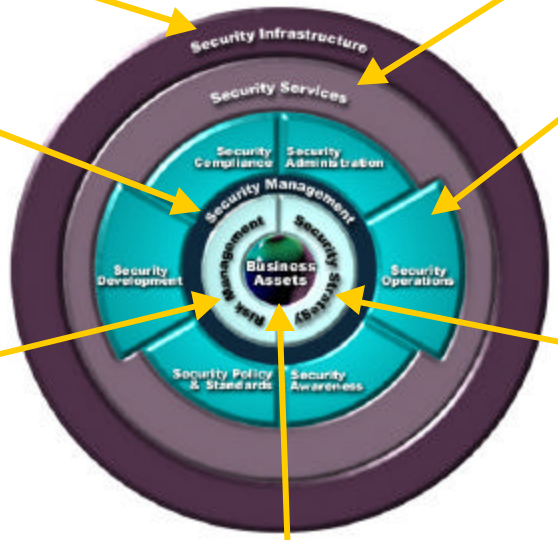
A security framework describes security areas and components to be considered when designing a security architecture (cont'd)

Department of Education

Security Infrastructure area consists of the actual security components which provide protection for the *Business Assets*. *Security Services* such as an authentication service are implemented using the security components in the *Security Infrastructure.*

Security Services consist of Security Base Services and ***Security Management***. Security Base Services are reusable components available to application developers to incorporate security functions such as authentication services into applications or business capabilities. *Security Management* has overall responsibility for the management of the secure enterprise.

Security Management initiates and manages enterprise-wide security programs to support the organization's business goals.



Core Capabilities comprise the security functions necessary to provide complete information security

Risk Management handles the overall security risks associated with business assets.

Security Strategy sets the future directions for information security and affects all areas of security within SFA.

Business Assets form the core of the *Security Framework* and are the data and processes that must be secured and protected.

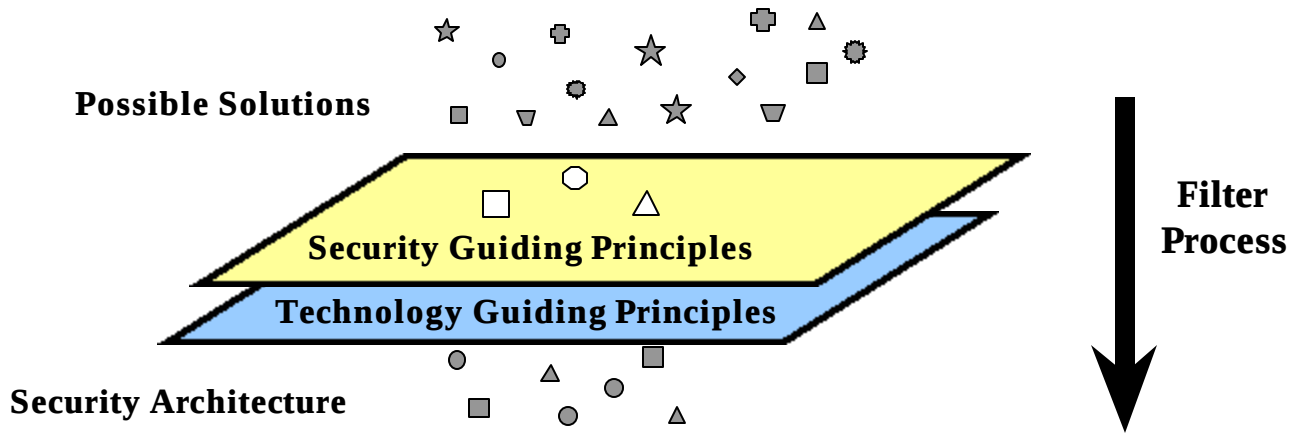
Contents

Department of Education

Security Guiding Principles

Department of Education

- The objective of Security Guiding Principles is to provide a filter so only the options that best meet the SFA security requirements and align with the technology architecture guiding principles are considered.
- Security Guiding Principles are policy statements that guide the security strategy and plan, secures the technical architecture, and ensure the linkage between the business initiatives, security requirements and security architecture. These policy statements are not rules that are applied individually, but represent long-term SFA security objectives.
- The following Technology Guiding Principles are based on analysis of SFA documents (i.e., EASI, Modernization Blueprint,) SFA personnel interviews as well as applying Andersen Consulting's best practices where appropriately aligned with the SFA vision.



Security Guiding Principles

- **Information Privacy -** ensures that security solutions are focussed on providing confidentiality of customers' personal information and business partners' sensitive business data, while ensuring easy access to data for authorized users.
- **Accountability** - ensures that roles and responsibilities of all individuals who interact with information are identified, defined, documented, and authenticated at a level commensurate with the established sensitivity and / or criticality of information systems and data.
- **Awareness** - ensures that SFA employees, customers, and business partners understand and accept the existence of security policies, practices and processes.
- **Multi-disciplinary** - ensures that policies, standards, processes and practices encompass as many relevant considerations and viewpoints as possible. At a minimum, legal, financial, organizational, operational, and technical considerations should be addressed.
- **Proportionality** - ensures that investments in security and privacy controls are justified by the risk to business assets. This means that all security investments must be supported by formal risk assessments. The risk assessment results will dictate the appropriate and proportional level of effort and cost that balance the value of the data, the controls and safeguards required, the probability of threat, and the potential for damage.

Security Guiding Principles

- **Integration** – ensures establishment of a system life-cycle whereby security is integrated as a part of all projects, from design through implementation through continuous improvement.
- **Timeliness** – ensures the right solution at the right time by implementing both a Security Incident Process and establishing a team to address global security incidents.
- **Separation of Duty** - ensures that no individual or group of individuals have privileges, accesses, or functions that would allow them to circumvent or manipulate control points within networks, systems, security environments or processes.
- **Continuity** – ensures that the security architecture supports the need for business continuity through provisions for change in employee roles, training, and disaster recovery.
- **Policy-Centered Security** – ensures documentation and application of policies, standards, and processes as a foundation for planning, controlling, and evaluating information security activities. This principle really drives all the other principles and forces a top-down documentation philosophy to be enforced.

Next Steps - Security Projects (Modified Risk Assessment)

Modified risk assessments focussed on defining risks and recommendations in the evolving environment for business units

Department of Education

Project

- Risk Assessment

Objective:

- Identify security & privacy risks and methods for addressing risks
- Provide security focussed project assistance for:
  - FMS implementation
  - Direct loan servicing re-engineering
  - Enhanced aid origination & funds disbursement
  - Infrastructure deployment (Internet R 1.0, Data Warehousing and EAI)

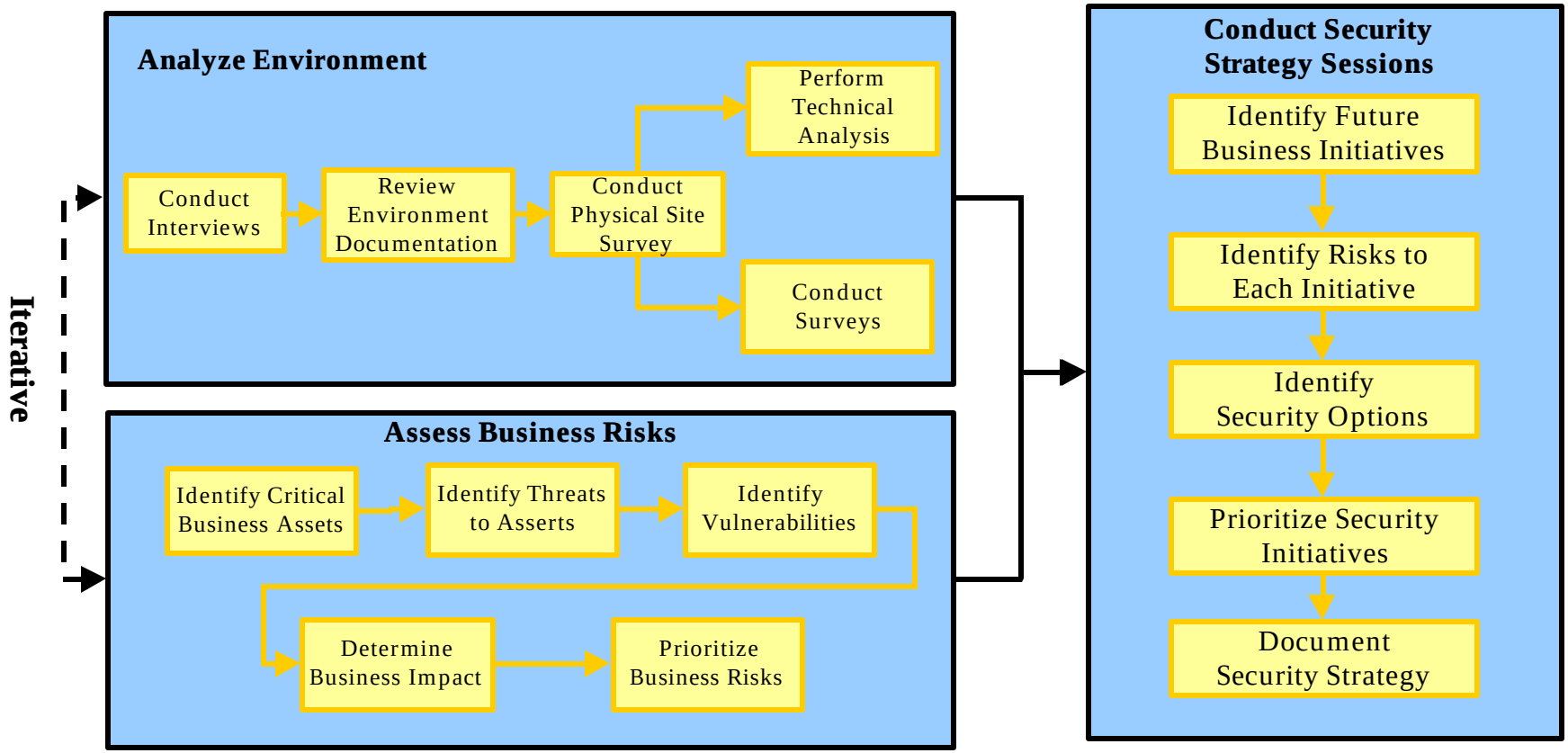
Deliverable:

- Risk assessment analysis and recommendations for the four major initiatives and core business processes
- Risk assessment methodology & toolkit
- Detailed vulnerability assessment
- Work plan for security projects
  - Short-term
  - Long-term

A risk assessment methodology that generates an SFA security strategy balancing business risks with asset value and cost to mitigate risks

Department of Education

Risk Assessment Approach



- Collaborative approach between Andersen Consulting; SFA business units, IT and security personnel
- Emphasis on business risks mitigation using a combination of security technology and processes
- Long-term security strategic planning based on identified business initiatives

A security organization ensures that information security issues are addressed throughout SFA business and IT processes

Department of Education

Project

- Security & Privacy Organization Design

Objective:

- Ensure that an organization is in place to support the security requirements of current and future business initiatives

Deliverable:

- High level gap analysis to determine areas in need of improvement throughout the security lifecycle.
- Map identified areas of concern to best practices to determine points of process breakdown.
- Next steps

High-level goals that the SFA Information Security organization should achieve

Department of Education

- Consolidation of Information Security and recovery functions into a single organization
- Appropriate corporate visibility for the security & privacy organization
- Minimal potential Operational / Information Security conflicts of interest
- Ownership over its budget
- Clearly defined roles and responsibilities ensuring:
  - creation / maintenance of information security policies
  - consolidation of security products evaluation and architecture consultant services
  - dedicated career path for security professionals
  - accountability and security awareness communication
  - inter-agency work and cooperation with schools and financial partners
  - resolution tracking for security weaknesses and audit recommendations
  - appropriate security incidents handling

Next Steps - Security Projects (Security Policies & Procedures)

A security policy communicates the importance of information assets and the level of commitment that SFA requires to protect these assets.

Department of Education

Project

- Security & Privacy Policies and Procedures

Objective:

- Define key policies & procedures and syndicate with SFA business units and systems administrators

Deliverable:

- Identify security policies & procedures documentation that needs to be added and / or up-dated to support new and current practices.
- Develop key security policies & procedures
- Define process to create, deliver, and maintain documentation.

Next Steps - Security Projects (Security Communication Plan)

A security communication plan must explains how to convey the right message, from the right communicator, to the right audience, through the right channel, at the right time

Department of Education

Project

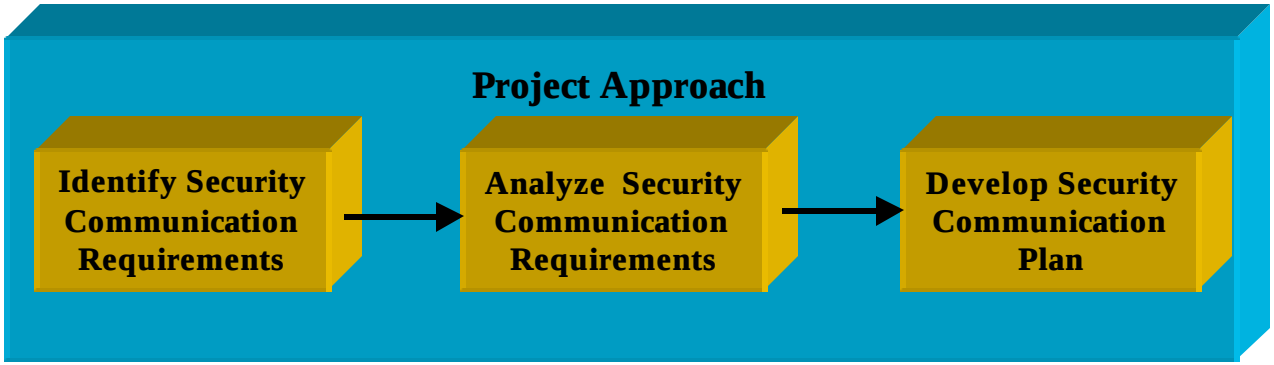
- Security & Privacy Communication Plan

Objective:

- Coordinate with SFA university and the Director of Communications to ensure that key security messages are communicated to SFA employees and business partners

Deliverable:

- Defined security & privacy awareness and communication plan
  - Address the six basic elements of communications: communicator, message, communication channel, feedback mechanism, receiver / audience, and time frame



SFA should have a security & privacy architecture that incorporates the security guiding principles needed to support the SFA business initiatives

Department of Education

Project

- Enterprise Security & Privacy Architecture

Objective:

- Define the hardware and software required to support a security & privacy architecture that protects SFA information assets

Deliverable:

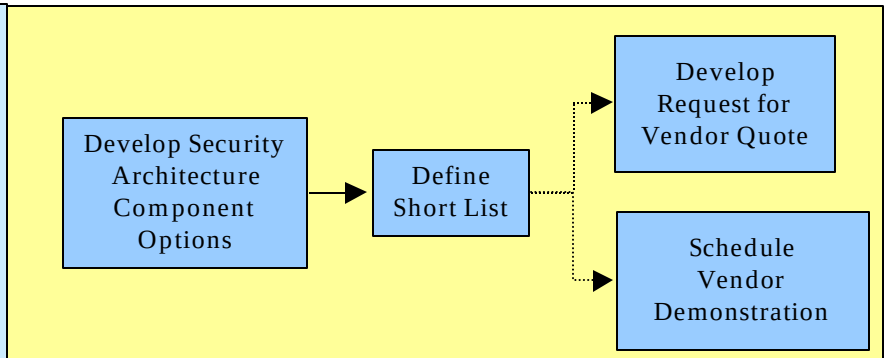
- Security & Privacy Architecture Design
  - Identify Security & Privacy Architecture Components
    - Technology Components
    - Security Processes
  - Select Security & Privacy Architecture Components
  - Design and Validate Security & Privacy Architecture

A structured approach to the architecture design ensures that all SFA security & privacy requirements are satisfied

Department of Education

Identify Security & Privacy Architecture Components

- Create short list of security & privacy architecture components that meet the qualifications set by the security architecture components requirements
  - Considers the execution, development, and operations architecture, as well as applications being delivered
  - Considers result of risk assessment
  - Considers cost effectiveness



Select Security Components

- Criteria is heavily based on whether the component can meet the security requirements
- Component may be part of overall technology architecture

Design and Validate Security & Privacy Architecture

- High-level security & privacy architecture design
- Validate security & privacy requirements are met by architecture design
- Fully documented security & privacy architecture design
- Documented security architecture standards